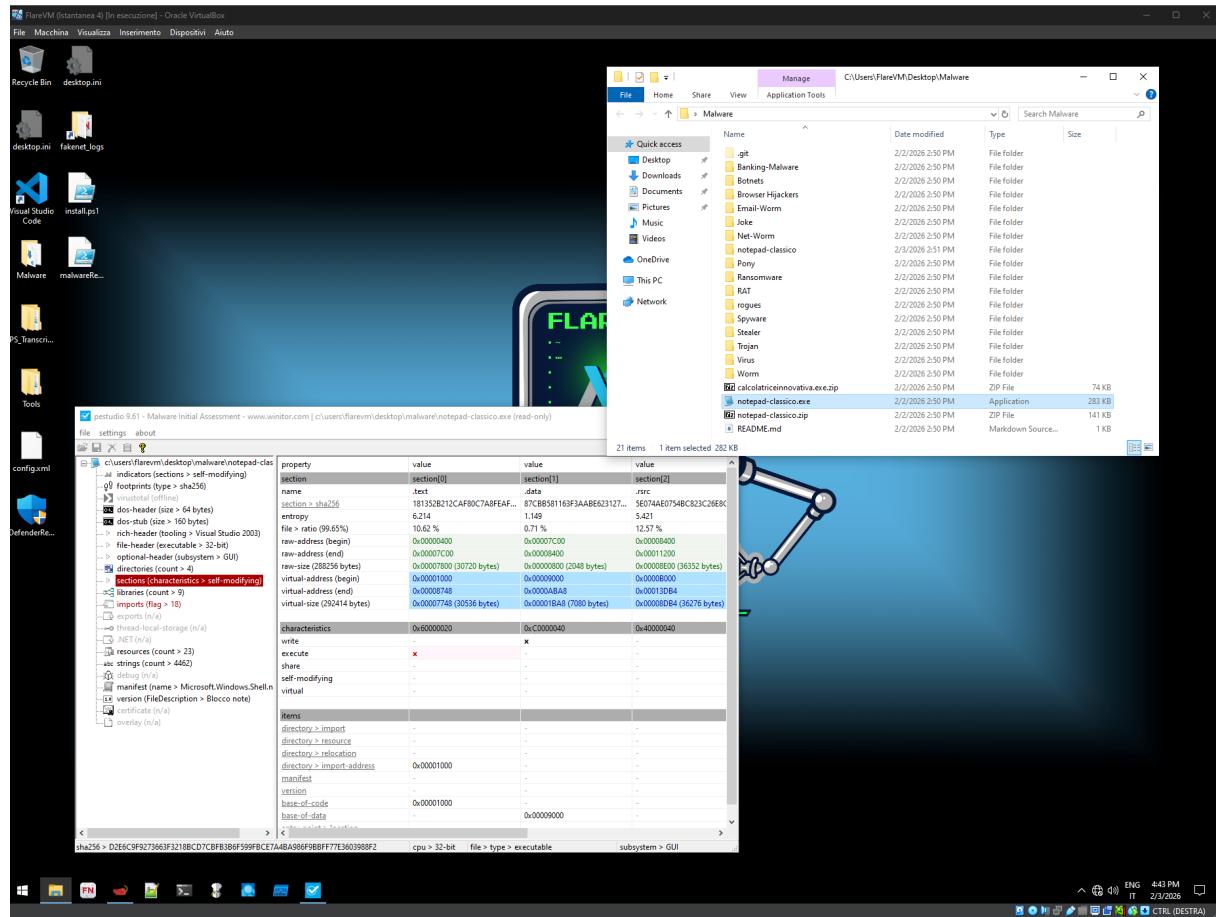


# Report Tecnico: Malware Analysis Statica

Target: File Eseguibile "notepad-classico.exe"

**Autore:** Josh Van Edward D Abanico  
**Data:** 3 febbraio 2026



**Obiettivo:** Analisi delle Librerie (Imports) e delle Sezioni (PE Headers)  
**Strumenti Utilizzati:** FlareVM, PEStudio

# Indice

<b>1</b>	<b>Introduzione e Obiettivi</b>	<b>2</b>
1.1	Scenario . . . . .	2
1.2	Hash del File . . . . .	2
<b>2</b>	<b>Fase 1: Analisi delle Librerie (Imports)</b>	<b>2</b>
2.1	Librerie Standard . . . . .	2
2.2	Funzioni Sospette e Flag Critici . . . . .	3
<b>3</b>	<b>Fase 2: Analisi delle Sezioni (PE Headers)</b>	<b>3</b>
3.1	Anomalie Rilevate . . . . .	3
<b>4</b>	<b>Conclusioni</b>	<b>4</b>

# 1 Introduzione e Obiettivi

## 1.1 Scenario

L'obiettivo di questa attività è analizzare un file sospetto denominato `notepad-classico.exe`. Il file si presenta come un comune editor di testo, ma è sospettato di contenere funzionalità malevole nascoste. L'analisi è stata condotta in un ambiente isolato (FlareVM) utilizzando tecniche di analisi statica.

## 1.2 Hash del File

- **Nome File:** `notepad-classico.exe`
- **Contesto:** Esercitazione Malware Analysis

# 2 Fase 1: Analisi delle Librerie (Imports)

## 2.1 Librerie Standard

L'analisi preliminare tramite **PEStudio** mostra che il malware importa diverse librerie standard di Windows per simulare un comportamento legittimo. Sono presenti `comdlg32.dll` e `SHELL32.dll`, che forniscono le finestre di dialogo "Apri/Salva" e funzionalità di Drag & Drop, tipiche di un Notepad reale.

pestudio 9.61 - Malware Initial Assessment - www.winitor.com   c:\users\flarevm\Desktop\malware\notepad-classico.exe (read-only)							
file	settings	about					
imports (201)	flag (18)	type	ordinal	first-thunk (IAT)	first-thunk-original (INT)	library	
<code>SetAbortProc</code>	-	implicit	-	0x81E8B55	0x00040B58	<code>GDI32.dll</code>	
<code>CreateCW</code>	-	implicit	-	0xFF8CCCCC	0x00040B4C	<code>GDI32.dll</code>	
<code>GetTextExtentPoint32W</code>	-	implicit	-	0xCCCCCC00	0x00040B34	<code>GDI32.dll</code>	
<code>StartPage</code>	-	implicit	-	0x04C25DED	0x00040B28	<code>GDI32.dll</code>	
<code>DeleteDC</code>	-	implicit	-	0xEB404004	0x00040B1C	<code>GDI32.dll</code>	
<code>EndDoc</code>	-	implicit	-	0x7509F983	0x00040B12	<code>GDI32.dll</code>	
<code>AbortDoc</code>	-	implicit	-	0x66067420	0x00040B06	<code>GDI32.dll</code>	
<code>EndPage</code>	-	implicit	-	0xF9836608	0x00040AFC	<code>GDI32.dll</code>	
<code>UnhandledExceptionFilter</code>	-	implicit	-	0xCCCC0004	0x00040AD6	<code>KERNEL32.dll</code>	
<code>MapViewOfFile</code>	x	implicit	-	0xC25D5EF	0x00040AC6	<code>KERNEL32.dll</code>	
<code>MultiByteToWideChar</code>	-	implicit	-	0xC7884747	0x00040AB0	<code>KERNEL32.dll</code>	
<code>UnmapViewOfFile</code>	x	implicit	-	0x0274FEB3	0x00040A9E	<code>KERNEL32.dll</code>	
<code>GetACP</code>	-	implicit	-	0xE375C985	0x00040A94	<code>KERNEL32.dll</code>	
<code>DeleteFileW</code>	x	implicit	-	0x6608B66	0x00040A86	<code>KERNEL32.dll</code>	
<code>SetEndOfFile</code>	-	implicit	-	0x01001244	0x00040A76	<code>KERNEL32.dll</code>	
<code>GetUserDefaultUILanguage</code>	-	implicit	-	0x15FF05F8	0x00040A5A	<code>KERNEL32.dll</code>	
<code>FormatMessageW</code>	-	implicit	-	0x8802759C	0x00040A48	<code>KERNEL32.dll</code>	
<code>LocalReAlloc</code>	-	implicit	-	0xF9836606	0x00040A38	<code>KERNEL32.dll</code>	
<code>WideCharToMultiByte</code>	-	implicit	-	0x743AF983	0x00040A22	<code>KERNEL32.dll</code>	
<code>SetLastError</code>	-	implicit	-	0x662374C6	0x00040A12	<code>KERNEL32.dll</code>	
<code>WriteFile</code>	x	implicit	-	0x8BFEB857	0x00040A06	<code>KERNEL32.dll</code>	
<code>GetLastError</code>	-	implicit	-	0xC9856606	0x000409F6	<code>KERNEL32.dll</code>	
<code>LocalSize</code>	-	implicit	-	0x8866C933	0x000409EA	<code>KERNEL32.dll</code>	
<code>IstrcpnW</code>	-	implicit	-	0x0875B856	0x000409DE	<code>KERNEL32.dll</code>	
<code>MulDiv</code>	-	implicit	-	0xEC885FF	0x000409D4	<code>KERNEL32.dll</code>	
<code>IstrcmpW</code>	-	implicit	-	0x88CCCCCC	0x000409C8	<code>KERNEL32.dll</code>	
<code>GetFileAttributesW</code>	-	implicit	-	0xCCC001C	0x000409B2	<code>KERNEL32.dll</code>	
<code>FindFirstFileW</code>	x	implicit	-	0xC2FFFFF	0x000409A0	<code>KERNEL32.dll</code>	
<code>FindClose</code>	-	implicit	-	0x1FB0060A	0x00040994	<code>KERNEL32.dll</code>	
<code>IstrcatW</code>	-	implicit	-	0xCCCCCCCC	0x00040988	<code>KERNEL32.dll</code>	
<code>GetCommandLineW</code>	-	implicit	-	0xCC0004C2	0x00040976	<code>KERNEL32.dll</code>	
<code>GetProcAddress</code>	-	implicit	-	0xC9000054	0x00040964	<code>KERNEL32.dll</code>	
<code>GetCurrentProcessId</code>	x	implicit	-	0x34E85B01	0x0004094E	<code>KERNEL32.dll</code>	
<code>IstrcmpW</code>	-	implicit	-	0x096241D	0x00040942	<code>KERNEL32.dll</code>	
<code>CreateFileW</code>	-	implicit	-	0x895E5F01	0x00040934	<code>KERNEL32.dll</code>	
<code>ReadFile</code>	-	implicit	-	0x0096203D	0x00040928	<code>KERNEL32.dll</code>	
<code>IstrcpW</code>	-	implicit	-	0x89FC4D8B	0x0004091C	<code>KERNEL32.dll</code>	
<code>CloseHandle</code>	-	implicit	-	0xD6FF5000	0x0004090E	<code>KERNEL32.dll</code>	
<code>FoldStringW</code>	-	implicit	-	0x00040B68	0x00040900	<code>KERNEL32.dll</code>	
<code>LocalLock</code>	-	implicit	-	0x016A51FF	0x000408F4	<code>KERNEL32.dll</code>	
<code>CompareStringW</code>	-	implicit	-	0xFFFFEC8D	0x000408E2	<code>KERNEL32.dll</code>	

Figura 1: Librerie grafiche e di interfaccia utente.

## 2.2 Funzioni Sospette e Flag Critici

Approfondendo l'analisi della Import Address Table (IAT), PEStudio segnala numerosi **Red Flag** su funzioni critiche, in particolare nelle librerie KERNEL32.dll e ADVAPI32.dll.

Le funzioni più rilevanti identificate sono:

- **Gestione File e Memoria (KERNEL32.dll):**
  - DeleteFileW: Permette al programma di eliminare file dal disco. Comportamento anomalo per un editor di testo, spesso usato dai malware per cancellare le proprie tracce (self-deletion).
  - MapViewOfFile / UnMapViewOfFile: Utilizzate per mappare file in memoria. Queste API sono spesso sfruttate per tecniche di *Process Injection* (es. Process Hollowing).
- **Persistenza (ADVAPI32.dll):**
  - RegCreateKeyW / RegSetValueExW: Funzioni che permettono di scrivere nel Registro di Sistema. I malware le utilizzano per garantirsi la **persistenza**, aggiungendosi alle chiavi di avvio automatico (es. *Run keys*).
- **Monitoraggio (USER32.dll):**
  - SetWinEventHook: Può essere usata per intercettare input dell'utente (comportamento simil-keylogger).
  - GetForegroundWindow: Permette di sapere quale finestra l'utente sta utilizzando, tecnica usata dai banking trojan.

## 3 Fase 2: Analisi delle Sezioni (PE Headers)

L'analisi delle sezioni rivela anomalie strutturali che indicano che l'eseguibile è stato manipolato o "impacchettato" (Packed).

### 3.1 Anomalie Rilevate

Dalla tabella delle sezioni emergono i seguenti indicatori di compromissione:

1. **Duplicazione delle Sezioni:** Sono presenti sezioni con nomi duplicati (es. due sezioni .text e due .rsrc), indicando una possibile iniezione di codice post-compilazione.
2. **Permessi RWX (Sezione .text critica):** La sezione identificata come section[3] (.text) presenta permessi simultanei di **Scrittura (Write)** ed **Esecuzione (Execute)**.
  - Questa configurazione viola le policy di sicurezza standard ( $W^X$ ).
  - Permette al codice di modificarsi durante l'esecuzione (Polimorfismo).
3. **Alta Entropia:** La stessa sezione presenta un valore di entropia pari a **6.428**. Sebbene non altissimo, combinato con il flag *Self-modifying*, suggerisce la presenza di codice offuscato o compresso per evadere l'analisi antivirus.

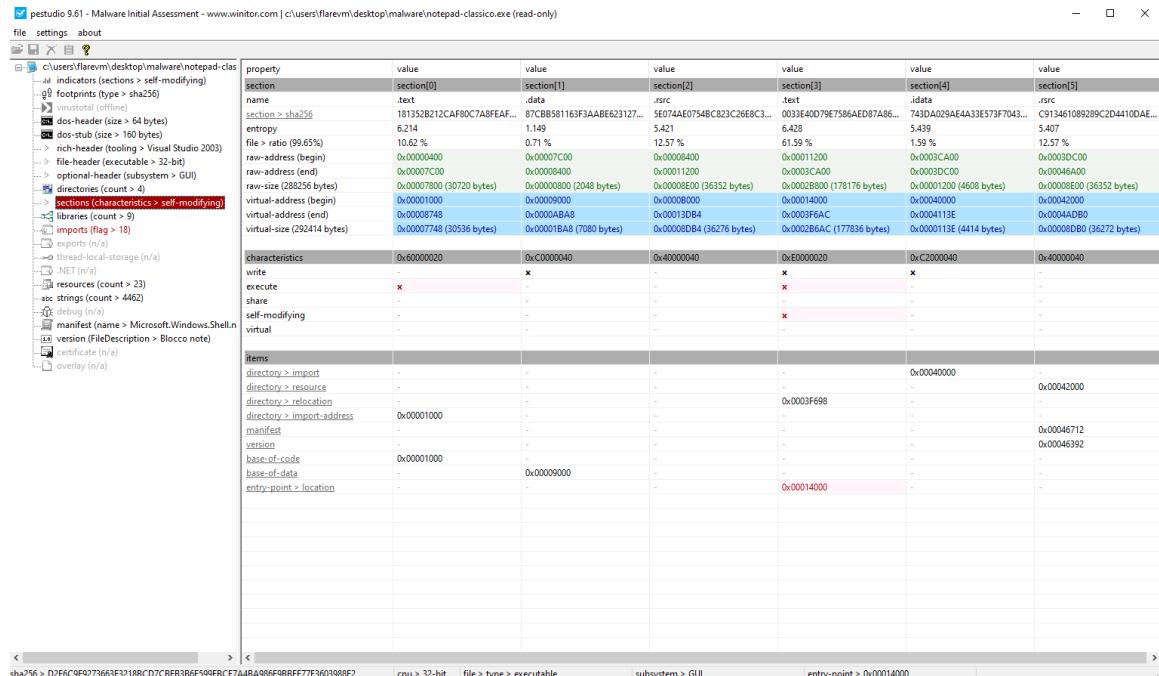


Figura 2: Analisi delle sezioni: evidenziati permessi RWX e flag self-modifying.

## 4 Conclusioni

L'analisi statica conferma che `notepad-classico.exe` non è un semplice editor di testo. Le evidenze raccolte mostrano:

- Capacità malevole:** Accesso al registro per persistenza, manipolazione file e memoria.
- Tecniche di evasione:** Struttura del file anomala (sezioni duplicate) e permessi RWX che suggeriscono l'uso di packer o codice polimorfico.

Si raccomanda di non eseguire il file in un ambiente di produzione e di procedere con l'analisi dinamica in Sandbox.